SPYWOLF

Security Audit Report

Completed on

June 8, 2022

MADE IN USA 🇺🇸

OVERVIEW

This audit has been prepared for **DEXMINER** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

SAFUFIDE

PROJECT DESCRIPTION

According to their website:

Dexminer NFT is a collection of 2,500 Dex Avatars. Each NFT is unique and living on the Binance Smart Chain. With hundreds of artistic elements, each avatar is crafted by DXM Team Artist.

DXM NFT collection uniquely interacts with the DXM Ecosystem. There are 5 rarities: Common, Rare, Epic, Super Epic & Exclusive. NFT Owners will receive BNB reward from 2% fee of $DXM sale volume, use NFT as a citizen to play DXM Social Game, AND trade the NFTs on the DXM NFT Marketplace.

Release Date: June 02, 2022

Category: Staking

CONTRACT INFO

Contract Name
DexMiner

Symbol
$DXM

Contract Address
0xb8C3Cd9B751B115826D7531550bE60f265e4868e

Network
Binance Smart Chain

Language
Solidity

Deployment Date
June 02, 2022

Verified?
Yes

Total Supply
10,000,000,000

Status
Launched

TAXES

Buy Tax
10%

Sell Tax
19%

*Fees can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of June 08, 2022)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxSellTxAmount	Additional Info
2,500,000	

rebaseFrequency
1800

LP Address(es)

Liquidity not added yet

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	10000000000 $DXM
Median Transfer Amount	10000000000 $DXM
Average Transfer Amount	10000000000 $DXM
First transfer date	2022-06-02
Last transfer date	2022-06-02
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2022-06-02 06:50:27 UTC
Created	2022-06-02 06:50:27 UTC
Create TX	0xa7956f4db28ee7b2c71807d9c7b3b125228740986f6e9ceea0ab007e080d06f5
Creator	0x10b67a030031819f03491ca0196b5e1b2bdbd0e1

FEATURED WALLETS

Owner address	0x10b67a030031819f03491ca0196b5e1b2bdbd0e1
Liquidity fee receiver	Same as owner
RiskFree value receiver	0x1351d3f4d8795cb8b3a2f0de7cc435d80466219d
Treasury receiver	0x10b67a030031819f03491ca0196b5e1b2bdbd0e1
LP address	**Liquidity not added yet**

TOP 3 UNLOCKED WALLETS

1

100% Same as owner

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

High Risk

This is rebase token with dynamic supply up to:
340,282,366,920,938,463,463,374,607,431,768,211,456.
Current supply is 10,000,000,000.
Owner can add whitelisted address and change next rebase time.
Whitelisted address can initiate manual rebase.

```
uint256 private constant MAX_SUPPLY = ~uint128(0);
10,000,000,000
340,282,366,920,938,463,463,374,607,431,768,211,456

function addWhitelisted(address account) public onlyOwner {
    _addWhitelisted(account);
}
function setNextRebase(uint256 _nextRebase) external onlyOwner {
    nextRebase = _nextRebase;
}
function manualRebase() external onlyWhitelisted{
    require(!inSwap, "Try again");
    require(nextRebase <= block.timestamp, "Not in time");

    uint256 circulatingSupply = getCirculatingSupply();
    int256 supplyDelta = int256(circulatingSupply.mul(rewardYield).div(rewardYieldDenominator));

    coreRebase(supplyDelta);
    manualSync();
}
```

Owner can set max allowed sell % amount from user's holdings. If set to 0 investors wont be able to sell.

```
function setTxFee(uint _addr) external onlyOwner {
    txfee = _addr;
}
function _transferFrom(address sender, address recipient, uint256 amount) internal returns (bool) {
.................
uint256 onePercent = balanceOf(sender).mul(txfee).div(100); //Should use variable
require(amount <= onePercent, "ERR: Can't sell more than 1%");
...........
}
```

FOUND THREATS

⚠ High Risk

Owner can disable trading, making it impossible to sell.

```
function setInitialDistributionFinished(bool _value) external onlyOwner {
    require(initialDistributionFinished != _value, "Not changed");
    initialDistributionFinished = _value;
}
function _transferFrom(address sender, address recipient, uint256 amount) internal returns (bool) {
bool excludedAccount = _isFeeExempt[sender] || _isFeeExempt[recipient];
require(initialDistributionFinished || excludedAccount, "Trading not started");
.......................
}
```

Owner can change max sell transaction limit, making it impossible to sell if set to 0.

```
function setMaxSellTransaction(uint256 _maxTxn) external onlyOwner {
    maxSellTransactionAmount = _maxTxn;
}
```

Owner can withdraw tokens from any address, including locking contracts, until launchmode is set to true.

```
function setLaunchModeFinished() external onlyOwner {
    launchMode = false;
}
function multiTransfer(address from, address[] calldata addresses, uint256[] calldata tokens)
 external onlyOwner {
    require(launchMode,"Cannot execute this after launch is done");
    require(addresses.length < 501,"GAS Error: max airdrop limit is 500 addresses");
    require(addresses.length == tokens.length,"Mismatch between Address and token count");
    uint256 SCCC = 0;
    for(uint i=0; i < addresses.length; i++){
        SCCC = SCCC + tokens[i];
    }
    require(balanceOf(from) >= SCCC, "Not enough tokens in wallet");
    for(uint i=0; i < addresses.length; i++){
        _basicTransfer(from,addresses[i],tokens[i]);
    }
}
```

FOUND THREATS

⚠ High Risk

Owner can set transfer fees up to 100%.

```
function setTransferTax(uint256 _transferTAX) external onlyOwner {
    transferTax = _transferTAX;
}
function takeFee(address sender, address recipient, uint256 gonAmount) internal returns (uint256){
.....
if(!automatedMarketMakerPairs[sender] && !automatedMarketMakerPairs[recipient]) {
    require(transferTax <= 100, "Wallet to wallet transfer disabled");
    feeAmount = gonAmount.mul(transferTax).div(100);
}
.....
}
```

FOUND THREATS

⚠ Medium Risk

Owner can change buy/sell fees up to 20% (combined buy+sell=40%).

```
uint256 public constant MAX_FEE_RATE = 20;

function setFees(uint256 _liquidityFee, uint256 _riskFreeValue,
uint256 _treasuryFee, uint256 _sellFeeTreasuryAdded,
uint256 _sellFeeRFVAdded, uint256 _feeDenominator) external onlyOwner {
    require(
        _liquidityFee <= MAX_FEE_RATE &&
        _riskFreeValue <= MAX_FEE_RATE &&
        _treasuryFee <= MAX_FEE_RATE &&
        _sellFeeTreasuryAdded <= MAX_FEE_RATE &&
        _sellFeeRFVAdded <= MAX_FEE_RATE,
        "wrong"
    );

    liquidityFee = _liquidityFee;
    buyFeeRFV = _riskFreeValue;
    treasuryFee = _treasuryFee;
    sellFeeTreasuryAdded = _sellFeeTreasuryAdded;
    sellFeeRFVAdded = _sellFeeRFVAdded;
    totalBuyFee = liquidityFee.add(treasuryFee).add(buyFeeRFV);
    totalSellFee = totalBuyFee.add(sellFeeTreasuryAdded).add(sellFeeRFVAdded);
    feeDenominator = _feeDenominator;
    require(totalBuyFee < feeDenominator / 4);
}
```

- Recommendation:
  - Good practice for fees deduction is combined buy+sell/transfer fees not to exceed 25%.

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

PROJECT NAME

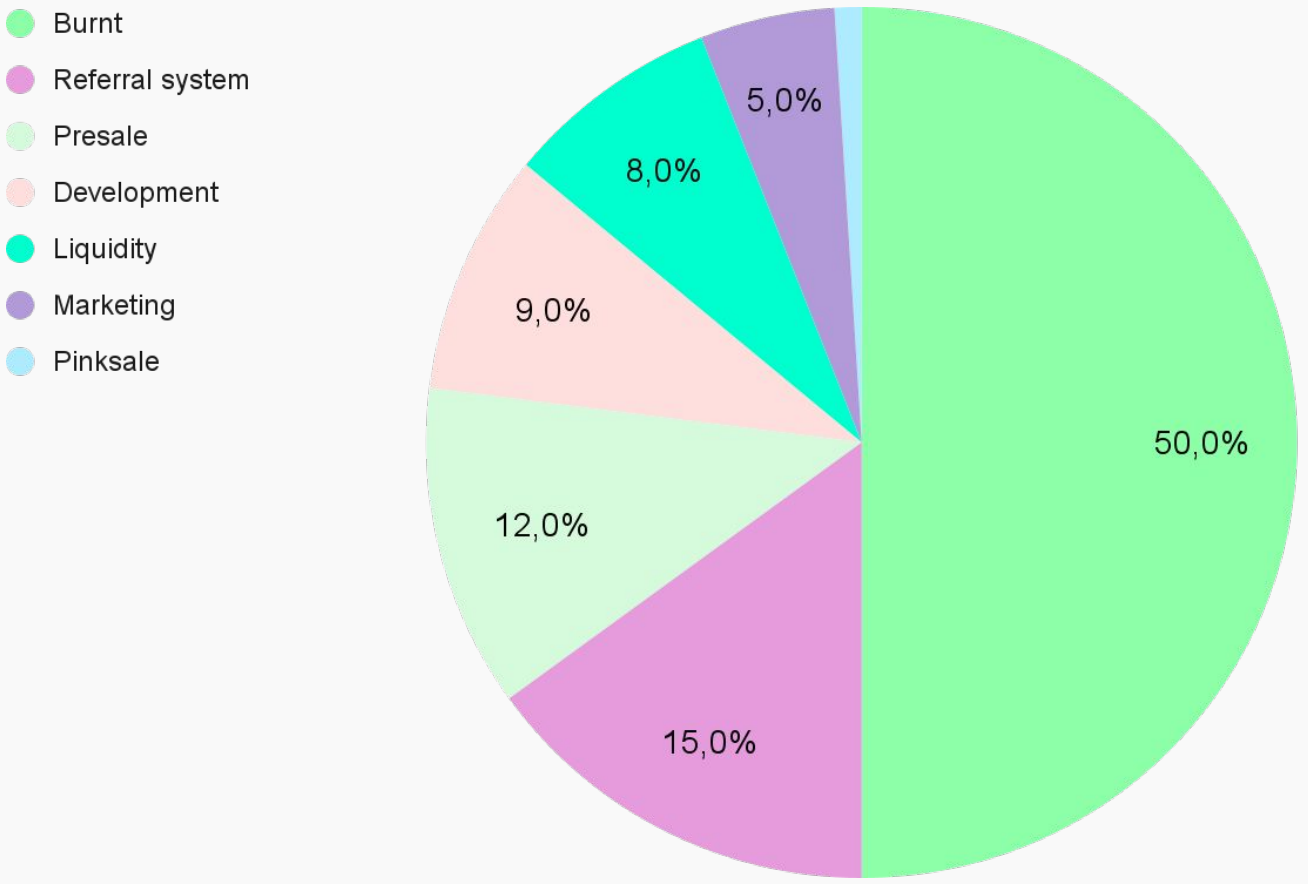
GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

*The following tokenomics are based on the project's whitepaper and/or website:

- 50% - Burnt
- 15% - Referral system
- 12% - Presale
- 9% - Development
- 8% - Liquidity
- 5% - Marketing
- 1% - Pinksale

Token Distribution



TOKENOMICS

THE TEAM

The team at DEXMINER has privately doxxed to SPYWOLF by completing the following KYC requirements:

- ID Verification
- Video statement
- Video interview with devs
- Owner's wallet verification

KYC INFORMATION

Issuer

SPYWOLF

Members

KYC Date

June 6, 2022

Format

Image

Certificate Link

https://github.com/SpyWolfNetwork/KYCs/blob/main/june/KYC_Dexminer_0xb8C3Cd9B751B115826D7531550bE60f265e4868e.png

WEBSITE

Website URL
https://www.dexminer.app/

Domain Registry
https://www.godaddy.com

Domain Expiration
Expires on 2023-05-24

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

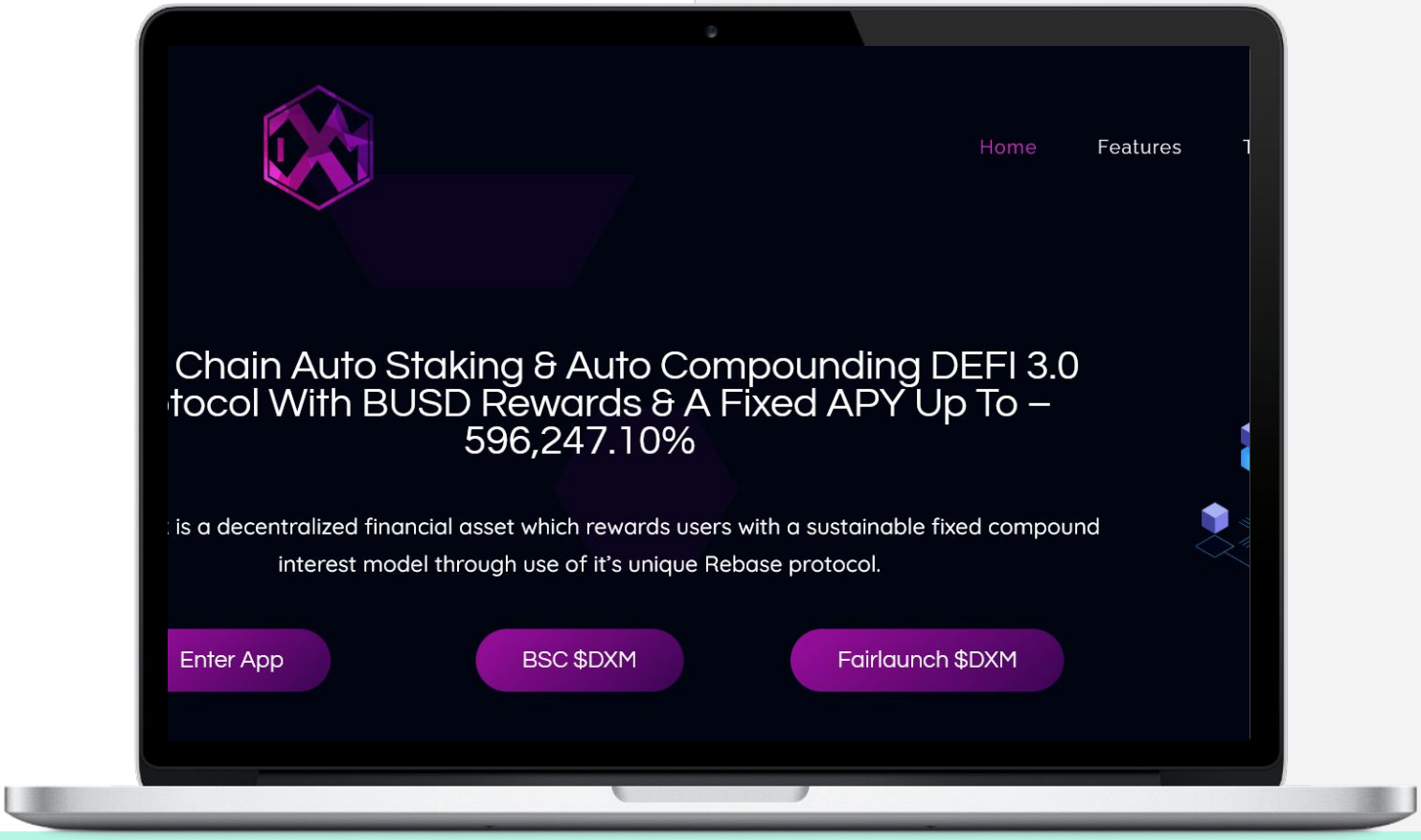
Design
Single page, template design, appropriate color scheme.

Content
Informative, no grammar mistakes.

Whitepaper
No whitepaper present. ⚠️

Roadmap
Yes, goals set at 5 phases without time frames

Mobile-friendly?
Yes



dexminer.app

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

The overall social media presence is OK. Some bots were added to Telegram to appear it has more followers. Not many active devs present.

Twitter

https://twitter.com/dexminerfinance

- 7 830 followers
- Active, all posts are made in 1 day period.
- Daily posts

Discord

https://discord.com/invite/cWzbeEpJEW

- 5 139 members
- No active members

Telegram

https://t.me/DEXMINER official

- 4.447 members, botted ⚠️
- No community interaction
- Only 1 response from each member ⚠️

Medium

https://medium.com/@dexminer

- 1 post with links to project's social pages

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.